Secure State Cyber: The importance of antivirus software and contingency planning for vessels

The final article in our cyber risks series, produced in collaboration with Secure State Cyber, focuses on the benefits of antivirus software, the importance of contingency plans in the event of a cyber-attack and what actions Members can take to ensure good security practice on board their vessels.

What are the benefits of employing antivirus software and why does it need to be kept updated?

The main purpose of an antivirus software is to check devices for viruses. Antivirus software achieves this by running scans on devices and looking for known viruses which are stored in its database. Cyber criminals are updating and re-configuring their virus every day with over 300 million new viruses having been created in 2018 alone. Therefore, for the antivirus software to look for the newest viruses, it must be regularly updated.

The benefits of having an updated well configured antivirus software are:

- Detection: The user will be notified if a virus is active on a device.
- Prevention: The device will be quarantined.

It must be kept in mind that an antivirus software is only effective when used consistently. Members should have a policy of regularly scanning storage devices and equipment prior to each time they are plugged in or integrated with the system. This policy should apply to all systems and personnel without exception.

It must also be noted that an antivirus doesn't completely prevent cyber threats and attacks. It is of paramount importance that the antivirus is supported by good policies and procedures.

What concerns should Members consider when developing contingency plans and drills for continual safe operations in the event of a cyber-attack?

Businesses and organisations that require nominal or close to no downtime during an event such as a significant cyber-attack, should develop and maintain a sound Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). These can also be extended to on board plans and procedures.

BCPs keep the organisation operational throughout an event which threatens normal functionality. A disaster recovery plan focuses on making a full or near-full recovery after a disaster has taken place. Both are equally important and each should be carefully planned. Once plans are developed, they should be regularly revisited, for any subsequent review or amendments.

It is imperative that: The documents are regularly updated and;

- The plans are tested regularly to determine their effectiveness in meeting their goals.
- The relevant employees are tested regularly to determine their effectiveness in the role they play in a disaster scenario. Table-top exercises and round table reviewing and assessing of the BCP and DRP should be carried out on a regular basis.

Is it important to regularly change the WI-FI password?

This is an essential step to maintaining good security practice. It is recommended that the non-guest Wi-Fi password is changed every six months, or at least annually.

Furthermore, it is recommended that the following Wi-Fi password policies are implemented:

- More than 25 characters
- Do not use dictionary words
- Have at least one lowercase letter, uppercase letter, number and symbol
- Temporarily block a user after five failed attempts to log in, we recommend a block time of 15 minutes
- Use WPA2 with AES

Crucially, in the case of admin access to Wi-Fi routers, it must be ensured that the Admin user name and password are changed from the default setting and that these details are shared with as few people as possible.

Should Members run periodic run checks to ensure that the systems are up to date and not infected/vulnerable?

Performing regular checks is a great way of lowering the risks. If system expertise is not available within the organisation, experts can be consulted to perform periodic checks of systems and networks for vulnerabilities. This is known as vulnerability scanning and can be performed by most cyber security companies.

In the cybersecurity industry, vulnerability scanning is a sub-task of the larger performance of vulnerability management.

Should Members have a relevant set of checklists to help crew comply with cyber procedures?

It is vital that all crew are aware of the risks and have the necessary tools, knowledge to fulfil a pivotal cybersecurity role. Therefore, having a checklist, is recommended to assist the crew in carrying out their cyber related duties on board as appropriate.

To complement the checklists, a robust cybersecurity awareness training program might also be of value. Considerations can be made to formulate ‘playbooks’ and checklists for crew to review and be aware of the proper procedures in an easy and understandable format. There should be clear and in-depth policies and procedures for everything allowed and specifically not allowed on board and the crew should also be regularly tested on these procedures.

This article is one in a series produced in partnership with cyber security specialists, Secure State Cyber.